REMARKS

Claims 15 to 29 are now pending.

Applicants respectfully request reconsideration of the present application in view of this response.

35 U.S.C. § 102(b) – Taylor reference

Claims 24 and 29 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,703,952 to Taylor ("Taylor reference").

The Taylor reference purportedly concerns a method and apparatus for generating a cipher stream. Title. The Taylor reference refers to a system for encrypting and decrypting a digital message having a linear driving subsystem 4 for generating a pseudo random data sequence, a nonlinear feedback system 6 for producing a cipher stream from the pseudo random sequence and an encryption processor 26 for encrypting or decrypting a message by combining it with the cipher stream. Abstract, lines 1-7. The Taylor reference further refers to the nonlinear feedback subsystem as having a nonlinear feedback processing means 10 for generating a feedback sequence 12 by applying a nonlinear function to at least one value from the pseudo random data sequence and at least one previous value of the feedback sequence, and a cipher stream generating means for generating a cipher stream by summing products of pairs of values of the pseudo random data sequence together with a value from the feedback sequence, the pairs of values being chosen such that the difference in sequence position as between each member of a pair is different as between each pair. Abstract, lines 8-18.

In contrast, claim 24 of the present application is directed to a device for loading input data into a program when performing an authentication using a cryptographic MAC function, including a first counter; a linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register, and for influencing an output of the linear feedback shift register using the first counter, the linear-feedback shift register forming at least part of a circuit; at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable.

The Taylor reference does not identically describe each feature of claim 24, including placement of each feature as claimed, as it must for anticipation. The Office Action cites col. 3, line 65 to col. 4, line 30, which refers to a cipher stream generator 2 having a linear driving

subsystem 4 and a nonlinear combining subsystem 6, the linear driving subsystem 4 includes a plurality of linear feedback shift registers 8 prestored with key data, outputs from the registers 8 are received by the nonlinear processor 10 of the nonlinear combining subsystem 6, the nonlinear processor 10 including a feedback system 12 having memory bits. The Taylor reference further states that the output 14 from the nonlinear combining subsystem 6 produces a data sequence which includes the cipher stream. Id. The Taylor reference does not identically describe the system as in claim 24 including at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable. Claim 29 depends from claim 24 and is allowable for at least the same reasons as claim 24. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 24 and 29; Applicants respectfully submit that claims 24 and 29 are allowable over the Taylor reference.

35 U.S.C. § 103(a) – Schilling and Taylor references

Claims 15 to 23 were rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent Application No. 2001/0030236 published on October 18, 2001 (long after Application foreign filing date of 1996) (continued from a line of applications, the earliest being filed on October 6, 1992, now U.S. Patent No. 5,359,182) to Schilling ("Schilling reference") in view of the Taylor reference.

The Schilling reference purportedly concerns a wireless telephone debit card system and method using a radio unit. Title and Abstract, line 1. The Schilling reference refers to a card reader reading information from a card, the read information includes a telephone number stored on the card. Abstract, lines 2-3. The Schilling reference further refers to a transceiver as transmitting a signal including the read telephone number to a base station, the transceiver receiving calls directed to the read telephone number; the first signal enabling the wireless communication system to direct calls for the read telephone number to the radio unit. Abstract, lines 4-8.

The Taylor reference purportedly concerns a method and apparatus for generating a cipher stream. Title. The Taylor reference refers to a system for encrypting and decrypting a digital message having a linear driving subsystem 4 for generating a pseudo random data sequence, a nonlinear feedback system 6 for producing a cipher stream from the pseudo random sequence and an encryption processor 26 for encrypting or decrypting a message by

combining it with the cipher stream. Abstract, lines 1-7. The Taylor reference further refers to the nonlinear feedback subsystem as having a nonlinear feedback processing means 10 for generating a feedback sequence 12 by applying a nonlinear function to at least one value from the pseudo random data sequence and at least one previous value of the feedback sequence, and a cipher stream generating means for generating a cipher stream by summing products of pairs of values of the pseudo random data sequence together with a value from the feedback sequence, the pairs of values being chosen such that the difference in sequence position as between each member of a pair is different as between each pair. Abstract, lines 8-18.

Claim 15 of the present application is directed to a method for loading input data into a program when performing a cash transaction authentication between and electronic cash chip card and a security module, the chip card including a stored credit balance, including the steps of debiting a requested cash amount from the chip card using a security function; adding and storing the requested cash amount in a cash amount summing counter of the security module, subdividing the input data into a plurality of data blocks; loading the plurality of data blocks into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter; introducing at least one additional feedback into the linear-feedback shift register following the at least one downstream counter; and switching off the at least one additional feedback after a predefined first number of pulses of an associated clock.

The Schilling and Taylor references, alone or in combination, do not describe or suggest all of the features of claim 15, including at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable. Applicants respectfully submit that the Schilling and Taylor references are not properly combinable, given that they are both directed to different subject matters and that no motivation is seen in either reference to suggest that they could be combined. The Schilling reference, as discussed above, concerns itself with chip and magnetic cards which can store information. The Taylor reference, as discussed above, appears to concern itself with generation of a cipher stream by a particular method.

Claims 16 to 23 depend from claim 15 and are allowable for at least the same reasons as claim 24. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 15 to 23; Applicants respectfully submit that claims 15 to 23 are allowable over the

Schilling and Taylor references.

Moreover, to reject a claim as obvious under 35 U.S.C. § 103, the prior art must disclose or suggest each claim element and it must also provide a motivation or suggestion for combining the elements in the manner contemplated by the claim. (See Northern Telecom, Inc. v. Datapoint Corp., 908 F.2d 931, 934 (Fed. Cir. 1990), cert. denied, 111 S. Ct. 296 (1990); In re Bond, 910 F.2d 831, 834 (Fed. Cir. 1990)).

In view of the prior amendments and above remarks, Applicants respectfully request allowance of claims 15 to 29.

CONCLUSION

In view of all of the above, it is believed that the objections to the drawings and Specification, and the rejections of claims 15 to 29, under 35 U.S.C. §§ 102(b) and 103(a), have been obviated, and that the currently pending claims are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

The Examiner is respectfully encouraged to contact the undersigned via telephone if such communication might advance allowance of the present application.

Respectfully submitted, By: Reg. No. 47084

Dated: June 7, 2004

By: Richard L. Mayer
Richard L. Mayer (Reg. No. 22,490)

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200

CUSTOMER NO. 26646